AMENDMENTS TO THE CLAIMS

Claims 1-22 are pending.

1. (Currently Amended) A method of authenticating a client to one or more computing devices ~~device~~ on ~~a Wi-Fi~~ one or more communications networks, the method comprising the steps of:

obtaining, by the client, a computing device identifier associated with a computing device ~~an access point identifier at a computing device, wherein said access point identifier identifies an access point of a Wi-Fi communications network~~;

selecting, at said client ~~computing device~~, a set of authentication parameters associated with said ~~access point~~ computing device identifier, said authentication parameters being stored in a tamper-resistant physical token operatively coupled to said client, said tamper-resistant physical token further permanently storing a unique identifier associated with said client, said tamper resistant physical token further storing a first cryptographic key; and

implementing an authentication process employing said set of authentication parameters, the authentication process comprising the steps of:

transmitting, by the client to the computing device, a first challenge, wherein said first challenge comprises an encrypted first random number and said unique identifier associated with said client, said first random number being generated inside said tamper-resistant physical token, said encrypted first random number being encrypted with said first cryptographic key;

receiving, by the client from the computing device, a second challenge, wherein said second challenge comprises an encrypted second random number, said second random number generated at said computing device and encrypted with a second cryptographic key, said second cryptographic key being obtained by said computing device and associated with said computing device identifier; and

permitting, at said client, said client to access said communications network via said computing device if said authentication process results in a successful authentication of said client.

2. (Currently Amended) The method of claim 1, wherein said computing device ~~access point~~ identifier is a basic service set identifier (BSSID).

3. (Cancelled)

4. (Cancelled)

5. (Currently Amended) The method of claim 1 [[4]], further comprising the step of installing said tamper-resistant physical token at said client ~~computing device~~.

6. (Currently Amended) The method of claim 5, wherein said tamper-resistant physical token is adapted to be inserted into a communications port at said client ~~computing device~~.

7. (Currently Amended) The method of claim 1 [[4]], wherein said tamper-resistant physical token further comprises one or more additional sets of authentication parameters, wherein ~~each set~~ each of the one or more additional sets of authentication parameters is associated with a unique computing device ~~access point~~ identifier.

8. (Currently Amended) The method of claim 7, wherein each of said unique computing device identifier ~~access point identifiers~~ is stored in said tamper-resistant physical token and in relation to an ~~its~~ associated set of authentication parameters.

9. (Cancelled)

10. (Cancelled)

11. (Cancelled)

12. (Currently Amended) The method of claim 1 ~~11~~, wherein said unique identifier is a serial number of said tamper-resistant physical token.

13. (Currently Amended) The method of claim 1 ~~11~~, wherein said set of authentication parameters further comprises:

a network receive cryptographic key, and

a network send cryptographic key.

14. (Currently Amended) The method of claim 13, further comprising the steps of:

encrypting, by the client, said first challenge with said network send cryptographic key; and

decrypting, by the client, said second challenge with said network receive cryptographic key.

15. (Currently Amended) A ~~communications~~ system for authenticating a client to one or more computing devices on one or more communications networks, the system comprising:

one or more computing ~~authentication~~ devices,

~~one or more~~ a client ~~devices~~, wherein the ~~each~~ client ~~device~~ is operatively coupled to ~~includes~~ a unique tamper-resistant physical token, the tamper-resistant physical token comprising:

one or more unique sets of authentication parameters, wherein each set of authentication parameters is associated with one or more of said one or more computing ~~authentication~~ devices;

a first cryptographic key, wherein said first cryptographic key is permanently stored in said tamper-resistant physical token;

a random number generator; and

a unique identifier ~~serial number~~, wherein said unique identifier is permanently stored in said tamper-resistant physical token; and

software installed in said client configured to cause said client to:

obtain a unique identifier of one of said one or more computing devices;

select a set of authentication parameters from said one or more unique sets of authentication parameters associated with the one of said one or more computing devices;

transmit, by the client to the one of said one or more computing devices, a first challenge, wherein the first challenge comprises an encrypted first random number and said unique identifier, wherein the first random number is generated by said random number generator within said unique tamper-resistant physical token, wherein said encrypted first random number is encrypted using the first cryptographic key;

receive, by the client from the one of said one or more computing devices, a second challenge, wherein the second challenge comprises an encrypted second random number, said second random number generated at the one of said one or more computing devices and encrypted using a second cryptographic key, said second cryptographic key being obtained by the one of said one or more computing devices and associated with the one of said one or more computing devices; and

permit, at said client, said client to access said communications network via the one of said one or more computing devices if the one of said one or more computing devices successfully responds to the first challenge and the client successfully responds to the second challenge.

16. (Currently Amended) The system of claim 15, wherein each client device further includes a wireless communications transceiver to communicate with one of said one or more computing devices ~~authentication device~~ via a wireless channel.

17. (Original) The system of claim 16, wherein said wireless channel is an IEEE 802.11 wireless channel.

18. (Currently Amended) The system of claim 15, wherein one or more computing ~~authentication~~ devices are Wi-Fi access points.

19. (Original) The system of claim 18, wherein at least two Wi-Fi access points are associated with different Wi-Fi networks.

20. (Original) The system of claim 19, wherein each of said one or more unique sets of authentication parameters is associated with an access point identifier.

21. (Original) The system of claim 20, wherein said access point identifier is a basic service set identifier (BSSID).

22. (Original) The system of claim 15, wherein each tamper-resistant physical token is adapted to be installed via a communications port at said client ~~computing device~~.